

Прозрачная голограмма – действительно хороший способ защиты от подделок. Разрушаемый стикер наносится сверху на подпись должностного лица и печать университета, что не дает возможности скопировать подпись.

Методом лазерной гравировки логотип выжигается лазером в отражающем слое голограммы. В этом месте наклейка становится прозрачной, и сквозь логотип виден материал, на который наклеена голограмма. В качестве дополнительной степени защиты можно применить и сквозную нумерацию голограмм. На каждую наклейку в заказанном тираже наносится индивидуальный номер. Это может быть буквенная серия, порядковый номер или любое другое сочетание. Сохранение информации о номере голограммы, времени и месте производства или продажи экземпляра продукции, на который она наклеена, существенно снижает возможность мошенничества в области поддельвания фальшивых дипломов и т. п.

Отметим достоинства использования голограмм на дипломах образования: оригинальность, улучшенный дизайн, имидж университета, эксклюзивность, защита диплома от подделки, повышение престижа БГЭУ, возможность стать лидером среди вузов, средство рекламы, возможность выпускнику ощутить причастность к научно-образовательному прогрессу.

Собственные голограммы должны быть зарегистрированными.

В настоящее время голография продолжает активно развиваться, и с каждым годом в этой области появляются новые интересные решения. Нет сомнения, что в будущем изобразительной голографии предстоит занять в жизни людей еще более значительное место.

<http://edoc.bseu.by>

Ю. В. Тимошенко

Научный руководитель – кандидат физико-математических наук, доцент Н. В. Шамукова, БФ БГЭУ (Бобруйск)

ИНФОРМАЦИОННЫЕ СИСТЕМЫ В ПРОМЫШЛЕННОСТИ И ИХ БЕЗОПАСНОСТЬ

Термин «информационная безопасность» (ИБ) не так давно вошел в широкое употребление, хотя деятельность современного предприятия невозможно представить без персональных компьютеров. На крупных предприятиях существуют специальные службы, в задачи которых входит обеспечение ИБ, выявление, локализация и устранение угроз ИБ предприятия. Они используют специальное дорогостоящее программное и аппаратное обеспечение, подчас настолько сложное в обслуживании, что требуется особая подготовка персонала для работы с ним.

Говоря о системах безопасности, нужно отметить, что они должны не только ограничивать допуск пользователей к информационным ресурсам, но определять и делегировать их полномочия в совместном решении задач, выявлять аномальное использование ресурсов, прогнозировать аварийные ситуации и устранять их последствия, гибко адаптируя структуру в условиях отказов, частичной потери или длительного блокирования ресурсов, т. е. защищать информацию на предприятии от различных угроз, которые,

воздействуя на информацию, могут привести к уничтожению, искажению, копированию, несанкционированному распространению информации, к ограничению или блокированию доступа к ней, что может привести к серьезным нежелательным последствиям.

Целью реализации информационной безопасности какого-либо объекта является построение Системы обеспечения информационной безопасности данного объекта (СОИБ). Для построения и эффективной эксплуатации СОИБ необходимо осуществить ряд мероприятий.

Рассмотрим информационную безопасность на примере предприятия ОАО «Белшина», информационное обеспечение которого представлено функционирующей единой базой знаний, которую составляет таблицы dbf, база Oracle и база 1С. В таблицах dbf хранятся данные по нормированию, составу готовой продукции, отпускным ценам, первичным документам движения готовой продукции. База Oracle хранят в себе данные отдела кадров и частично отиза. А в базе 1С дублируются данные по движению готовой продукции и содержатся первичные документы по движению всех материальных ценностей. На предприятии также используется база данных (БД) правовой информации: «Эксперт», НАУ 9, Информационная система «Кодекс», «Главбух-Инфо».

База данных на ОАО «Белшина» обладает тремя важными свойствами:

1. БД хранится и обрабатывается в вычислительной системе. То есть, любые внекомпьютерные хранилища информации ими данных не являются.
2. Данные в БД хорошо структурированы (систематизированы).
3. Структура БД обеспечивает эффективный поиск и обработку данных.

Но при проведении анализа информационной системы ОАО «Белшина» были выявлены критические точки процесса, а именно:

- бесперебойное энергообеспечение;
- бесперебойная работа оборудования;
- регулярное резервное копирование данных;
- управление сетевыми ресурсами;
- организация разграничения доступа к информационной системе;
- организация конфиденциальности информации.

С учетом недостатков процесса было предложено добавить в систему обеспечения информационной безопасности работу «Обеспечение сохранности данных», исключить остановку частично или полностью функционирования информационной системы в результате отказа одного или нескольких компонентов, повысить защищенность и управляемость системы безопасности сетевой инфраструктуры.